## REMARKS

This amendment is in response to the Office Action dated August 19, 2005. Claims 1-36 are pending in the application, including independent claims 1, 26, 32 and 34-36. Claims 1-36 stand rejected. New claims 37 and 38 are added.

### I. Drawings

The drawings filed on February 5, 2002 were objected to by the Examiner. However, the Examiner left the Applicant's representative Daniel Burns a phone message on Nov. 11, 2005, indicating that this objection was in error and is now moot.

### II. Claim Objections

Claims 32 and 36 are objected to because of the following informalities: on line 7 of the respective claims, replace "single skeleton" with "single skeleton key."

The Applicant has amended the claims per the Examiner's recommendation.

### III. Claims rejected under 35 U.S.C. § 112

*A. Claim 2 stands rejected under 35 U.S.C. § 112, first paragraph.*

The Examiner asserted that "[c]laim 2 recites the limitation of storing the encrypted document decryption key in the document; however the specification only discloses storing the encrypted document decryption key in the encrypted document (see Specification, pg. 3, last paragraph)."

The Applicant respectfully disagrees and notes that the cited portion of the Specification does not discuss "storing" of encrypted document decryption keys. Rather, the cited portion describes an encrypted document 12 having embedded in it one or more encrypted versions of a document decryption key 14.

Nevertheless, claim 2 has been amended to clarify the antecedent basis of "the document" on line 1.

*B. Claim 1 stands rejected under 35 U.S.C. § 112, second paragraph.*

The Examiner pointed out that claim 1 recites the limitation "the document" in line 7 with insufficient antecedent basis for this limitation in the claim.

The Applicant has amended claim 1 to correct this oversight.

## IV. Claims rejected under 35 U.S.C. § 101

Claims 1-36 stand rejected under 35 U.S.C. § 101. According to the Examiner, "[i]n view of Applicant's disclosure, specification pg. 20, lines 7-9, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., hardware implemented) and intangible embodiments (e.g., software, propagated signal)."

The Applicant respectfully disagrees with the Examiner. However, in order to expedite prosecution of the Application, claims 1, 26, 32 and 34-36 have been amended to clarify their statutory basis.

## V. Claims rejected under 35 U.S.C. § 102

*A. Claims 1, 2, 8, 10, 13, 23-25 and 34 stand rejected as being anticipated by U.S. Pat. No. 6,336,189 ("Takeda").*

Claim 1 recites associating a first key with an encrypted document decryption key, the encrypted document decryption key being associated with an encrypted document. The encrypted document decryption key, when decrypted, yields a document decryption key usable to decrypt the encrypted document. The first key is usable to decrypt the encrypted document decryption key and is provided in an access controlled manner to users for use in opening the encrypted document.

Takeda discloses a data capsule 1000 that contains an encrypted version of data 100, a verification means 200 that communicates with an external proving device to obtain proof data, a usage controls means 300 that enables use of the data 100, and a decryption means 400 for decrypting the data 100. *See* Takeda, *Abstract* and FIG. 1. The cited portion of Takeda discloses an embodiment that addresses a security concern that arises when a data encryption key is stored in the data capsule 1000 since "the data capsule can possibly be analyzed to take out the decryption key and data decrypted with the decryption key can be used illegally." *See* Takeda, col. 4, lines 58-62.

Takeda teaches that a data encryption key *k* is encrypted by an RSA-based public key *E*, where *E* and the encrypted data encryption key *k* are stored in the verification means of 200 of the data capsule 1000. *See* Takeda, col. 5, lines 1-17 and FIG. 6. The key *k* can be decrypted by a private key *D*. *See* Takeda, col. 5, lines 28-52. However, to prevent users from obtaining access to *D*, it is stored in a secret key hold means 2023 within the proving device 2000. *See id.* The encrypted data encryption key *k* is provided to the external proving device 2000 by the verification means 200, decrypted using private key *D* by decryption means 2022 within the proving device 2000, and then sent back to the verification means 200. *See id.* Thus, *D* is not provided to, or accessible by, end users. Assuming for argument's sake that *D* is analogous to the first key of claim 1, it follows that <u>Takeda does not teach or suggest providing the first key in an access controlled manner to users</u>.

For at least this reason, the Applicant respectfully submits that claim 1 is in condition for allowance.

Claims 2, 8, 10, 13, 23-25 and 34 incorporate elements similar to those of claim 1 and are allowable for at least the same reason.

## VI. Claims rejections under 35 U.S.C. § 103

### *A. Claims 3-7, 11, 32, 33 and 36 stand rejected over Takeda in view of U.S. Pat. No. 6,069,957 ("Richards").*

Claim 3 recites encrypting a first key and associating with the encrypted first key a second key that can be used to decrypt the encrypted first key. The second key is provided in an access controlled manner to users for use in opening all documents that can be opened through use of the first key.

Richards discloses a restricted-access television system where decryption keys are used to decrypt program material. *See* Richards, *Abstract*. The cited portions of Richards teach that a key (SK) is encrypted by a first key (PK), which is encrypted by a second key (CUSTOMER_CODE). *See* Richards, col. 9, lines 14-17. But Richards teaches that the CUSTOMER_CODE is "not available to the customer." *See* Richards, col. 10, lines 36-37. Moreover, "the CUSTOMER_CODE is extremely well concealed and can change with time." *See* Richards, col. 10, lines 59-63. Accordingly, the relied upon portion of Richards does not teach or suggest providing the second key in an access controlled manner to users. This deficiency is not remedied by Takeda.

Furthermore, claim 3 depends from claim 1. As discussed above, Takeda does not teach or suggest providing the first key in an access controlled manner to users, as required by claim 1. Richards does not remedy this deficiency in Takeda. FIG. 14 in Richards illustrates a decryption system within a customer decoder. The only user accessible part of the decryption system is the user controlled part 115 of the User Encryption Variable (UEV) register 112, which holds a UEV key. *See* Richards, col. 11, lines 1-13. The user-controlled part 115 is entered by the user by setting DIP switches, for example. *See* Richards col. 11, lines 4-5. The user controlled part 115 is combined with two other parts, both of which are not accessible to the user, to form the UEV key. *See* Richards, col. 11, lines 4-13. Thus, the UEV key is not provided to the user. Nor is it used to decrypt a key which can then be used to decrypt content – this is the responsibility of a downstream key (SK). However, the downstream key (SK) is not accessible by the user. *See* Richards, col. 11, lines 14-21. Accordingly, Richards does not teach or suggest providing a first key in an access controlled manner to users as required by claim 1.

Claims 3-7 and 11 depend from claim 1 and are also allowable for at least that reason.

Claim 32 recites providing in an access controlled manner multiple skeleton decryption keys for multiple encrypted documents, where a single skeleton key can be used to open multiple encrypted documents, a single encrypted document can be opened using more than one skeleton key, and a single skeleton key can be opened using one or more other skeleton keys. Each single skeleton key is a key usable to decrypt one or more secondary decryption keys. Each secondary decryption key is a skeleton key or a decryption key for an encrypted document. One or more skeleton keys can be issued for a document or a set of documents, and a holder of a particular skeleton key can open any document to which the particular skeleton key applies, directly or indirectly.

As discussed above, Takeda and Richards do not teach or suggest providing user access to keys. Claim 32 is allowable for at least this reason.

Claims 33 and 36 incorporate elements similar to those of claim 32 and are allowable for at least the same reason.

B. *Claim 12 stands rejected over Takeda in view of Richards, and further in view of William Stallings, Cryptography and Network Security: Principals and Practice (2nd Ed. 1998) ("Stallings").*

Claim 12 depends from claim 1. As discussed above, Takeda and Richards fail to render claim 1 obvious. The cited portions of Stallings fail to sure the deficiencies in Takeda and Richards.

Accordingly, claim 12 is allowable for at least this reason.

C. *Claims 9 and 16 stand rejected over Takeda in view of the Examiner's Official Notice.*

The Examiner took Official Notice that "it is notoriously well known in the art for digital information to be stored in memory within a data file" and "digital data for the purpose of mass distribution often includes a user's agreement as well as licensing limitations that defines the extent of operation of the digital data."

Claims 9 and 16 depend from claim 1. As previously discussed, Takeda does not anticipate claim 1. Neither of the Examiner's Official Notices remedy the deficiency in Takeda.

Claims 9 and 16 are allowable for at least this reason.

D. *Claims 14, 15, 17, 26-29 and 35 stand rejected over Takeda in view of Stallings.*

Claims 14, 15, and 17 depend from claim 1. As previously discussed, Takeda does not anticipate claim 1. The relied upon portion of Stallings fails to cure the deficiency in Takeda.

Claims 14, 15 and 17 are allowable for at least this reason.

Claim 26 recites obtaining an encrypted electronic document and obtaining a collection of keys, the keys including keys that are encrypted. The keys and the document have associations defined between certain pairs of them, where each association of a pair consisting of a first key and an encrypted second key indicates that the first key can be used to decrypt and thereby make usable the second key, where each association of a pair consisting of an encrypted document decryption key and the encrypted document indicates that the encrypted document decryption key, when decrypted, can be used to decrypt the encrypted document, and where a user has access to and can use certain ones of the keys in the collection. Claim 26 also recites using the associations to identify at least one key in the collection that is usable, directly or indirectly, to open the encrypted document, and to which the user has access.

The Examiner stated that Takeda does not disclose keys and a document having associations defined between certain pairs of them. *See* Office Action mailed August 19, 2005, p. 15, #36. Yet the Examiner asserted that Takeda discloses using such associations to identify at least one key in a collection that is usable, directly or indirectly, to open an encrypted document. The cited portion of Takeda (col. 5, lines 20-24) reads as follows:

> The proving device 2000 operates on its authentication data reception means 2021 to receive the authentication data, operates on its decryption means 2022 to decrypt the authentication data using the private key D held by the private key hold means 2023, and sends the result as proof data to the data capsule. Specifically, the decryption means 2022 calculates the following formula (3).

The above quoted portion of Takeda describes receiving an encrypted decryption key *k* that has been encrypted with an RSA-based public key *E,* and decrypting it using a private key *D.* The decrypted key is then returned to verification means 200 where it can be used to decrypt data. The relied upon portion of Takeda does *not* disclose using associations to identify at least one key in a collection that is usable, directly or indirectly, to open an encrypted document. In contrast, the private key *D* is always used to decrypt *k*. Moreover, since the Examiner acknowledges Takeda does not disclose the keys and the document having associations defined between certain pairs of them, it follows that Takeda cannot teach or suggest using such associations.

The cited portion of Stallings describes sending an identifier Key ID for a public key $KU_b$ in a message containing encrypted data so that a receiver of a message knows what private key to use to decrypt a session key $K_s$. The session key can then be used to decrypt the message data. *See* Stallings, pp. 363-364 and Figure 12.3. As with Takeda, the relied upon portion of Stallings does not disclose using associations to identify at least one key in a collection that is usable, directly or indirectly, to open an encrypted document. Instead, the public key $KU_b$ is identified by its Key ID – not by an association of keys and a document – and is used to decrypt the session key $K_s$. *See* Stallings, p. 363.

Claim 26 is allowable for at least this reason.

Claims 27-29 and 35 incorporate elements similar to those of claim 26 and are allowable for at least the same reason.

## VII. Conclusion

In light of the above remarks, the Applicant respectfully requests reconsideration of the claim rejections and allowance of all claims.

By responding in the foregoing remarks only to particular positions taken by the examiner, the Applicant does not acquiesce with other positions that have not been explicitly addressed. In addition, the Applicant's arguments for the patentability of a claim should not be understood as implying that no other reasons for the patentability of that claim exist.

Please deduct $100 from deposit account 06-1050 for excess claims fees. Please apply any charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 18-Nov-2005

Daniel J. Burns
Reg. No. 50,222

Customer No.: 021876
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50312911.doc